Symantec™ Event Collector for Cisco PIX Implementation Guide

Version 1.0

Symantec™ Event Collector for Cisco PIX Implementation Guide

Documentation version 1.0

Copyright notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec Global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response collectors, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
EVENT COLLECTORS

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License.

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec, license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows:

You may:

A. use that number of copies of the Software as have been licensed to You by Symantec under a License Module for Your internal business purposes. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single machine.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use each licensed copy of the Software on a single central processing unit; and

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

F. use the Software to collect data from a type of technology other than when using a Symantec Event Manager product or another Symantec product designed for use with this Software that corresponds to that type of technology (i.e., antivirus, firewall, IDS, etc.) ; nor

G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content which is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates which Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and

limitations set forth above will apply regardless of whether you accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Export, re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Chapter 3 Using the collector

Chapter 1

Introducing Symantec™ Event Collector for Cisco PIX

This chapter includes the following topics:

About the product

Symantec Event Collector for Cisco PIX enables centralized, cross-tier logging, alerting, and reporting between the Symantec Enterprise Security Architecture (SESA™) event management system and the Cisco PIX Firewall. There is one collector for each Cisco PIX Firewall syslog server in a network.

The Symantec Event Collector for Cisco PIX retrieves events that are generated by PIX Firewalls and integrates these events into SESA. Currently, the events represent the operation of the PIX Firewall. These events are stored in the SESA DataStore (a database) where they are available for visual inspection as the basis for alert notifications and incident creation and as raw data for report generation. While the Symantec Event Collector for Cisco PIX is running, it monitors the syslog for new PIX events. Significant PIX events are translated into a single SESA event.

After you install Symantec Event Collector for Cisco PIX, the PIX Firewall is SESA-enabled. When a product is SESA-enabled, you can use the Symantec management console to view the events that it forwards to SESA. The Symantec management console provides a central location in which to view and manage the reporting of event data across multiple SESA-enabled security products.

How the Event Collector retrieves data

A SESA Agent must be installed on the same computer as the Symantec Event Collector for Cisco PIX. When you install the SESA Agent, you furnish a small set of initial parameters (the SESA Manager's IP Address and port). After you install the SESA Agent, you can change its default parameters using the SESA Manager.

See "Configuring the SESA Agent" on page 39.

The Symantec Event Collector for Cisco PIX links to the SESA Agent by way of the SESA Agent Application Library. This lets the SESA Agent securely log the events that it receives from the Symantec Event Collector for Cisco PIX to a SESA Manager. Because the PIX syslog can conceivably collect events from one or many firewalls, the PIX events that are forwarded to SESA can potentially originate from many sources.

When the SESA Manager is unavailable, the SESA Agent queues messages for later delivery, up to a default maximum of 2 MB. This queue size can be changed by using the Symantec management console to edit the maximum queue size value on the Logging tab of the SESA Agent configuration.

How the Event Collector processes events

All SESA events are a discrete instance of a class of similar events. An Event ID field indicates the exact instance. The Symantec Event Collector for Cisco PIX derives discrete event IDs and classifications by examining the contents of key fields. The Symantec Event Collector for Cisco PIX currently processes more than 100 signatures from the PIX Firewall into SESA events.

The Symantec Event Collector for Cisco PIX assigns one of the following categories to each event:

Security	Messages that come from the PIX syslog are assigned to the Security category.
Application	Events that are generated by the Symantec Event Collector for Cisco PIX are assigned to the Application category.

It also assigns each event one of the following severities:

Informational	Events that represent expected behavior
Warning	Events that represent suspicious behavior
Minor	Events that could require attention
Major	Events that require attention now
Critical	Events that need attention now with a broad range of application to the enterprise

Table 1-1 describes the events that the Symantec Event Collector for Cisco PIX generates.

Table 1-1 Symantec Event Collector for Cisco PIX events

Event	Category	Severity	Description
Application Start	Application	Informational	The Event Collector is starting.
Application Stop	Application	Informational	The Event Collector is stopping.

In the SESA environment, events that arrive from a SESA Agent are generally understood to be events that are generated by the system on which the SESA Agent is installed.

Because Symantec Event Collector for Cisco PIX is collecting events from a syslog that may receive events from multiple firewalls, the event data is structured to uniquely identify those systems.

Events from the Symantec Event Collector for Cisco PIX are logged as if they originated with the machine that logged the message to the PIX syslog. This value is found in the machine IP field. In addition, the machine name field in SESA is populated with the reporting PIX Firewall name.

About SESA

SESA (Symantec Enterprise Security Architecture) is an underlying software infrastructure that integrates multiple Symantec and third-party products to provide flexible control of security within organizations. Through SESA, these products protect your networked computing environment from malicious code, intrusions, and blended threats. You can monitor and manage security-related events through the Symantec management console.

You can use the Symantec management console to change the security configurations of integrated products (configuration options differ depending on the features of the integrated product). You can configure and tune SESA components to reflect the infrastructure and performance needs of your organization.

To minimize the complexity of managing many security technologies across numerous clients and users, SESA lets you group clients according to their security infrastructures and functional management needs. You can logically create groups of managed computers that are based on locations, products installed, areas of responsibility, or combinations. These organizational units help you better delegate event management, product configuration, and maintenance tasks.

The Symantec management console also provides role-based administration. You can create users and limit the actions that they can perform and the information that they can see. For example, users who have access to the event viewer and alert viewer can centrally manage attacks, threats, and exposures by correlating security information from integrated Symantec and non-Symantec anti-virus, firewall, intrusion detection, and vulnerability assessment products.

The Symantec management console helps you focus on threats that require your attention. You can query, filter, and sort data to reduce the security-related events that you see in the console. You can also configure alert notifications in response to events and generate, save, and print tabular and graphical reports of event status, based on filtered views that you have created.

For more information about SESA, see the *Symantec Enterprise Security Architecture Installation Guide* and the *Symantec Enterprise Security Architecture Administrator's Guide*.

Chapter 2

Installing the collector

This chapter includes the following topics:

Understanding the installation process

The Symantec Event Collector for Cisco PIX installs shared and product-specific components to send events to SESA. To enable the Symantec Event Collector for Cisco PIX to forward events to SESA, the installation process includes:

- Installing the SESA Integration Wizard
- Installing the Symantec Event Collector for Cisco PIX and the SESA Agent

Planning the SESA integration component setup

The first phase of installing the Symantec Event Collector for Cisco PIX is to extend the SESA functionality to use the Symantec Event Collector for Cisco PIX data.

To enable SESA support, install the SESA integration components for the Symantec Event Collector for Cisco PIX on the computer on which the SESA Manager is installed. Install the components by running a SESA Integration Wizard on the SESA Manager computer, which extends the SESA functionality to use the Symantec Event Collector for Cisco PIX. The extended functionality lets you centrally view and manage reports for PIX events in the Symantec management console.

You must also install the SESA Event Manager for Firewalls on the SESA Manager computer. This must be installed prior to installation of the Symantec Event Collector for Cisco PIX integration components on the SESA Manager.

Preparing to log data to the syslog server

The PIX Firewall must be configured to send log data to a remote syslog server.

This documentation assumes that a syslog server is already set up to receive PIX syslog messages. Instructions for setting up a syslog server are beyond the scope of this document.

To configure PIX to log to the syslog server, see "Configuring the PIX Firewall" on page 19. If the syslog server is running on a Solaris or Linux host, no further configuration is necessary. If the syslog server is running on a Windows host, ensure that the syslog daemon is configured to log using the BSD UNIX syslog format.

If the syslog daemon does not include an option for logging in BSD UNIX syslog format, find the logging format with the following structure:

```
MMM DD HH:MM:SS <PixIP> %PIX-<EventLevel>-<EventID>
```

where <PixIP> is the IP address of the PIX Firewall, <EventLevel> indicates the importance of the event, and <EventID> is the numeric code for the PIX log event.

If the syslog daemon cannot be configured to use this log format, use the Kiwi Syslog Daemon for Windows (http://www.kiwisyslog.com). This Windows syslog daemon supports the BSD UNIX syslog format.

Planning the Event Collector setup

The second phase of installing the Symantec Event Collector for Cisco PIX is to install the Event Collector for PIX. The Symantec Event Collector for Cisco PIX reads events from the PIX log, formats them, and sends them to the SESA Agent. The SESA Agent, which installs with the Symantec Event Collector for Cisco PIX, enables communication and configuration of events between SESA and the PIX Firewall. The collector must be installed on the same computer as the Cisco PIX syslog. To install the Event Collector, use the Symantec Event Collector for Cisco PIX Installation Wizard. This also installs the SESA Agent if one is not already installed.

The Symantec Event Collector for Cisco PIX installs components on:

- The SESA Manager to which PIX events are forwarded.
- The computer that collects PIX events from the syslog.

Installation requirements

Before you install the Symantec Event Collector for Cisco PIX, make sure the computer on which the SESA DataStore is installed has enough hard disk space to accommodate the additional security events that the Cisco PIX Firewall sends to it. In addition, make sure that the computer or computers where you plan to

install the collector meet the necessary requirements and that the following conditions have been met:

SESA	SESA version 1.1 is installed and operating properly. If you have a previous version of SESA, you must first uninstall it before you can install version 1.1. You cannot migrate previous versions of SESA to version 1.1 or reinstall over previous versions. Version 1.1 is not backward-compatible. The SESA Event Manager for Firewalls must be installed on the SESA Manager. For more information, see the *Symantec Enterprise Security Architecture Installation Guide*.
Cisco PIX Firewall	Firewall PIX version 6.2 /6.3 The Cisco product or products that you are integrating with SESA are installed and operating properly. For more information, see the Cisco PIX documentation.
Collector setup	The collector installation that you have selected and planned for is the optimal configuration for the PIX product to operate as a SESA-enabled product.

System requirements

The Symantec Event Collector for Cisco PIX and the SESA Agent must install on a computer with access to the PIX syslog.

Collector system requirements

The Symantec Event Collector for Cisco PIX installs the SESA Agent and the collector on the same computer. The computer on which you install the SESA Agent must meet the following minimum system requirements:

Operating system	Windows 2000 with SP3 (at least) Solaris 2.8/2.9
SESA version	SESA version 1.1
Sun Java requirements	Java Runtime Environment (JRE) version 1.3.1_02 JRE is not required if the collector is installed on the SESA Manager computer.

Processor	Intel Pentium-compatible 133-MHz processor
Memory	■ 32 MB of memory for the SESA Agent ■ 64 MB RAM for each Cisco PIX product (128 MB or more recommended)
Hard disk space	35 MB of hard disk space for Symantec collector framework program files. 95MB of hard disk space if the SESA Agent, JRE, and the PIX Collector are on one computer.
Network connection	TCP/IP connection to network

These requirements may be in addition to resources or requirements of PIX components that are running on the same system.

SESA Integration Components requirements

The SESA Integration Components for the Event Collector for Cisco PIX are installed on the SESA Manager computer. The SESA Integration Components require version 1.1 of SESA. If you have a previous version of SESA installed, you must uninstall it before you can install version 1.1. You cannot install version 1.1 over a previous version or migrate a previous version to SESA 1.1.

If you have more than one SESA-enabled product installed on a single computer, these products can share a SESA Agent. However, each product must register with the Agent. Consequently, even if an Agent has already been installed on the computer for another SESA-enabled security product, you must install the collector to register the particular Cisco PIX product with the Agent.

The SESA Agent is preconfigured to listen on IP address 127.0.0.1 and port number 8086. The Symantec Event Collector for Cisco PIX uses this information to communicate with the Agent. If you must change the IP address or port number for the Agent, you must do so through the Symantec management console. After an Agent is installed, it is controlled through the Symantec management console, even though it is running on the computer that is running the security product.

For more information, see the SESA documentation.

SESA Manager requirements

Before installing any components on the SESA Manager, ensure that it is installed and operating properly. For installation information, see the SESA documentation.

Install the SESA integration component for the Event Collector on the SESA Manager before you install the Event Collector.

Ensuring connectivity

By default, the Symantec Event Collector connects to the SESA Manager using the SESA Agent and HTTPS on port 443. You can configure a different port, if desired. Appropriate routing must exist between the workstation with the collector installed and the SESA Manager for event messages to reach the SESA Manager. In addition, make sure that there is no firewall or device policy blocking the connection between the Event Collector and the SESA Manager.

At a command prompt, type the following test command:

```
telnet <SESA-IP-ADDRESS> 443
```

<SESA-IP-ADDRESS> is the IP address of the SESA Manager. The connection should appear to hang but not be refused. After typing a few characters, there should be a message that the connection has been lost.

SESA datastore requirements

After you install the Event Collector and the SESA integration components, PIX can begin to forward events to SESA. The amount of disk space that you need to accommodate the event data depends on how many devices are logging events, how verbose they are, and how long you want to keep the event data in the database.

128GB should be sufficient to store events from several agents for 30 days. This number is in addition to disk space for other devices that may already be reporting to SESA. 128 GB of datastore can store 17-19 million PIX events.

Table 2-1 describes the suggested minimum size of the datastore based on the anticipated number of events received in 30 days.

Table 2-1 Minimum size of datastore based on data rate

Data rate	Number of events in 30 days	Minimum size of datastore
10 events per second	25,920,000	172 Gigs
30 events per second	77,760,000	518 Gigs
60 events per second	155,520,000	1036 Gigs
100 events per second	259,200,000	1728 Gigs

Installing the Event Collector components

The Event Collector gathers security information from the PIX Protection System. The Event Collector sends the information through the SESA Agent to the SESA Manager for storage in the SESA DataStore.

To complete installation

1. Ensure connectivity between the SESA Manager and the Symantec Event Collector for Cisco PIX.
2. Install the SESA Manager components. See "SESA Integration Components requirements" on page 17.
3. Install the Symantec Event Collector for Cisco PIX components.
   The Symantec Event Collector for Cisco PIX and the SESA Agent must install on the same computer.

Configuring the PIX Firewall

The PIX Firewall can be configured from the command line via Telnet, SSH, a direct serial connection, or the PIX Device Manager Web interface.

Configuring PIX syslog logging via a command line interface

1. Log in to the firewall.
2. To begin the configuration process, type the command:
   ```
   configure terminal
   ```
3. Enter the following command to identify the remote syslog server:
   ```
   logging host <interface> <ipaddress>
   ```

where <interface> is the firewall interface that is connected to the syslog server's network and <ipaddress> is the IP address of the remote syslog server.

By default, this configures the PIX Firewall to send log data to that IP address on UDP port 514.

If your syslog server has been configured to receive syslog data on another UDP port or TCP port, you must type the above command as follows:

```
logging host <interface> <ipaddress> <protocol>/<port>
```

where <protocol> is either TCP or UDP and <port> is the appropriate port number.

4 To configure the logging level, type:

```
logging trap <level>
```

where <level> is the appropriate logging level.

See "Selecting the appropriate logging level" on page 21.

5 To activate logging, type:

```
pix (config)# logging on
```

The firewall should now begin logging to the remote syslog server.

Configuring the PIX Firewall via web interface

1 Click the **System Properties** tab.

2 On the left side of the interface, expand the Logging menu.

3 Select **Syslog**.

4 Click **Add.**

5 Type the IP address of the remote syslog server.

6 Select the firewall interface that is connected to the syslog server's network.

7 Specify the protocol and port number on which the syslog server is listening for new connections.

In most cases, the default settings (UDP, port 514) are appropriate.

8 On the right side of the interface, click the **Level** menu.

9 Select the appropriate logging level.

See "Selecting the appropriate logging level" on page 21.

10 On the left side of the interface, select **Logging Setup**.

11 Select **Enable logging**.

12 Click **Apply to Pix** to apply the logging configuration changes.

The firewall should begin logging to the remote syslog server.

Selecting the appropriate logging level

PIX Firewall logging levels range from 0 (for emergency messages only) to 7 (the highest logging level, used primarily for debugging).

Each level is inclusive of those levels below it. For example, logging level 6 includes all log messages of severity 0-6.

When selecting the appropriate logging level, you must balance the need for detailed log information with additional network traffic and disk usage that are consumed by the log data.

The Symantec Event Collector for Cisco PIX functions regardless of the logging level selected. However, higher log levels provide the Symantec Event Collector for Cisco PIX with more data to analyze and report to SESA.

A logging level of 6 or 7 ensures maximum analysis of firewall activity.

If you select a lower logging level, be aware of the following restrictions:

- Logging level 6 or higher detects successful connection activity. If the logging level is set to 5 or lower, the Symantec Event Collector for Cisco PIX does not process and report successful connection activity.
- Logging level 5 or higher detects most firewall management events, such as remote management connections and changes to the firewall's saved configuration.
- Logging level 4 or higher detects most denied connections and dropped packets. These events are often important indicators of an attack or scan. For this reason, do not set the logging level lower than 4.

Installing SESA integration components

The SESA integration components for the Event Collector include reports that are specific to the Symantec Event Collector. You must run the SESA Integration Wizard for every SESA Manager that needs to process PIX events.

To install the SESA integration components

1. Install the Symantec Event Collector CD on a SESA Manager.
2. Click **Install Symantec Event Collector Integration Components**.
3. In the Welcome window, click **Next**.

4. In the Requirements dialog, verify that you have the SESA Manager running on this machine, then do one of the following:
   - If you have satisfied the requirements, click **Next**.
   - If you have not satisfied the requirements, click **Cancel**.

     The setup program closes so you can install the necessary files.
5. In the SESA Domain Administrator Information dialog box, do the following:
   - In the SESA Domain Administrator Name text box, type the name of the SESA Domain Administrator account.
   - In the SESA Domain Administrator Password text box, type the password for the SESA Domain Administrator account.
   - In the IP Address of SESA Directory text box, type the IP address of the computer on which the SESA Directory is installed (may be the same as the SESA Manager IP address if both are installed on the same computer).

     If you are using authenticated SSL instead of the SESA default, anonymous SSL, you must type the host name of the SESA Directory computer. For example, mycomputer.com.

     For more information on SESA default, anonymous SSL and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.
   - In the SSL Port text box, type the number of the SESA Directory secure port. By default, the port number is 636.
6. Click **Next**.
7. In the Ready to proceed dialog box, do one of the following:
   - If you are ready to proceed, click **Next**.
   - If you want to change your settings, click **Back**.
8. In the Configuring Your System dialog box, you see the progress of the configuration of the Symantec management console for the Symantec Event Collector for PIX. When it is complete, click **Next**.
9. In the Symantec management console Integration Status window, verify that your installation was successful, then click **Finish**.
10. Repeat steps 1 through 9 on each SESA Manager to which you are forwarding PIX events. To confirm successful installation, log on to the Symantec management console.
11. On the Events tab, select the appropriate datastore and navigate to the Firewall Event Family.

12 Open the Firewall Event Family.

13 Confirm that you have a new tab that is labeled Symantec Event Collector for Cisco PIX.

If you have this and the associated reports, your install of the integration components completed successfully.

Installing the Event Collector

If the computer is already running the current version of the SESA Agent, the installation program installs only the Symantec Event Collector for Cisco PIX.

Installing the Symantec Event Collector for Cisco PIX

If the SESA Agent is not installed, during the Symantec Event Collector for Cisco PIX installation, a SESA Agent Installation Information dialog box prompts you to specify the information that is needed to install it.

To install the Symantec Event Collector for Cisco PIX on Windows

1 On the computer with Cisco PIX syslog, log in as a user with Administrator rights/privileges.

2 Insert the Symantec Event Collector for Cisco PIX CD-ROM into the CD-ROM drive.

If the installation program does not start automatically, navigate to the CD-ROM drive and double-click **Install/setup_win32.exe**.

3 In the PIX Collector InstallShield Wizard Welcome dialog box, click **Next**.

4 Read the license agreement, select **I accept the terms of the license agreement**, and click **Next**.

5 Select **Symantec Event Collector for Cisco PIX Components**, and click **Next**.

6 Verify the requirements for this setup type, and click **Next**.

7 If the SESA Agent is not installed on your computer, the SESA Agent Install Information dialog box displays. Enter the installation directory and click **Next**. The default destination directory is given:

C:\Program Files\Symantec\SESA\Agent

8 In the SESA Agent Information dialog box, enter the values for the following fields:

- Primary SESA Manager IP Address is the SESA Manager to which the SESA Agent regularly directs events.

- Primary SESA Management Port (default is port 443)
- Secondary SESA Manager IP Address is the SESA Manager to which the SESA Agent directs events upon failure of the primary SESA Manager. If there is no Secondary SESA Manager installation, leave this field blank.
- Secondary SESA Management Port (default is blank). If there is no Secondary SESA Manager installation, leave this field blank.

9 Click **Next**.

10 The Custom Setup dialog box shows the default location where the Event Collector is installed:

C:\Program Files\Symantec\PIX Collector

Do one of the following:

- To install the Event Collector in the default location, click **Next**.
- To change the installation location for the Event Collector, click **Browse**.

In the Change Current Destination Folder dialog box, select a new location for the Event Collector, click **OK**, and then click **Next**.

11 In the Event Collector Information dialog box, enter the following information:

- Type the name of the Local PIX Logfile Path that the collector should be monitoring for Cisco PIX events. This is only the directory name.
- Type the name of the Local PIX Logfile Name that the collector should be monitoring for Cisco PIX events. This is only the filename.

12 Click **Next**.

13 Click **Next** for each of the summary screens.

14 In the InstallShield Wizard Completed dialog box, click Finish.

15 If you are prompted to restart your computer, do one of the following:

- To restart now, click **Yes**.
- To restart later, click **No**.

  Note: You do not have to immediately restart your computer.

To install the Symantec Event Collector for Cisco PIX on Solaris

1 On the computer with the Cisco PIX syslog, log in as the root user.

2 Mount the Symantec Event Collector for Cisco PIX CD-ROM.

3 Start the installation program by changing the current directory to the install directory on the CDROM and execute the following command:

```
./setup_solarissparc.bin
```

4. In the PIX Collector InstallShield Wizard Welcome dialog box, click **Next**.
5. Read the license agreement and select **I accept the terms of the license agreement**.
6. Click **Next**.
7. Select the setup type **Symantec Event Collector for Cisco PIX**.
8. Click **Next**.
9. Verify the requirements for this setup type and click **Next**.
10. If the SESA Agent is not installed on your computer, the SESA Agent Install Information dialog box displays. Enter the installation directory and click **Next**. The default destination directory is:

    `/opt/Symantec/SESA/Agent`
11. In the SESA Agent Information dialog box, enter the values for the following fields:
    - Primary SESA Manager IP Address is the SESA Manager to which the SESA Agent will direct events on a regular basis.
    - Primary SESA Management Port (defaults to 443).
    - Secondary SESA Manager IP Address is the SESA Manager to which the SESA Agent will direct events upon failure of the primary. If there is no Secondary SESA Manager installation, leave this field blank.
    - Secondary SESA Management Port (default is blank). If there is no Secondary SESA Manager installation, leave this field blank.
12. Click **Next**.
13. Enter the installation directory for the Event Collector. The default location installation location is:

    `/opt/Symantec/PixCollector`
14. Do one of the following:
    - To install the Event Collector in the default location, click **Next**.
    - To change the installation location for the Event Collector, click **Browse**.

      In the Change Current Destination Folder dialog box, select a new location for the Event Collector. Click **OK**, then click **Next**.

Note: Do not use spaces in the installation location on Solaris.

---

15 In the Event Collector Information dialog box, type the following information:

- Type the name of the local PIX logfile path that the collector should be monitoring for Cisco PIX events. This is only the directory name:

  ```
  /var/adm
  ```

- Type the name of the local PIX logfile name that the collector should be monitoring for Cisco PIX events. This is only the file name:

  ```
  messages
  ```

16 Click **Next**.

17 Click **Next** for each of the summary screens.

18 In the InstallShield Wizard Completed dialog box, click **Finish**.

19 If you are prompted to log out, do one of the following:

- If you ran the InstallShield process using the File Manager, then close the starting window. Log out and log back in.
- Log out and log back in.

Starting and stopping the Event Collector service

The Event Collector runs as a service/daemon on the host on which it is installed. To start and stop the Event Collector, you start and stop the service or daemon as necessary.

To start or stop a service on Windows

1. On the computer on which you installed the Event Collector, on the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Administrative Tools**.
3. In the Administrative Tools window, double-click **Services**.
4. In the Services dialog box, right-click the **Symantec Event Collector for PIX** service, then click **Start** or **Stop**.

To start or stop the Event Collector daemon on Solaris

1. On the computer on which you installed the Event Collector, log in as the root user.
2. Type the following command to start the Event Collector daemon:

   ```
   /etc/rc3.d/S99Collector start
   ```

3. Type the following command to stop the Event Collector daemon:

   ```
   /etc/rc3.d/S99Collector stop
   ```

To start or stop the SESA Agent daemon on Solaris

1. On the computer on which you installed the Event Collector, log in as the root user.
2. Type the following command to start the Event Collector daemon:

   ```
   /etc/rc3.d/S99sesagentd start
   ```

3. Type the following command to stop the Event Collector daemon:

   ```
   /etc/rc3.d/S99sesagentd stop
   ```

Verifying the installation

After the service is installed, you can verify that the appropriate components are installed and working properly. Look in Windows Services to ensure that the SESA Agent and SESA Collector are both listed.

Verify the installation

To verify the installation, do the following:

- Verify that the appropriate services have started.
- Verify that the Symantec Event Collector for PIX is displayed in the Symantec management console.
- Examine the Event Collector and SESA Agent logs as necessary.

To verify that the appropriate services have started on Windows

1. On the Event Collector computer, select **Programs** > **Control Panel** > **Administrative Tools** > **Services**.
2. In the Services window, verify that the following services are running:
   - Symantec Event Collector for PIX
   - SESA AgentStart Service

To verify that the appropriate services have started on Solaris

1. On the computer on which you installed the Event Collector, log in as the root user.
2. Type the following command to list the Event Collector daemon processes:

   ```
   ps –efu root | grep <installation path>
   ```

3. In the list of processes shown, verify that the following processes are running:
   - Symantec Event Collector for PIX

     ```
     opt/Symantec/PixCollector/bin/run-service.sh
     ```

   - SESA AgentStart Service

     ```
     opt/Symantec/SESA/Agent/agentd -START
     ```

To verify that the Event Collector is displayed in the Symantec management console

1. On the SESA Manager computer, on the Windows taskbar, click **Start** > **Programs** > **Symantec Enterprise Security** > **SESA Console**.
2. Log on to the Symantec management console using a SESA user account with sufficient rights to view SESA configurations.

   The SESA user must belong to a role that has rights to the SESA-enabled Symantec Event Collector for PIX product.
3. On the Events view tab, expand **Symantec Enterprise Security** > **SESA DataStore** > **Firewall Event Family**.

4 Under Firewall Event Family, verify that the Symantec Event Collector for Cisco PIX folder is listed and contains the following reports:
   - All PIX Events
   - PIX Events (last 8 hours)
   - PIX Events (last 24 hours)
   - PIX Events (last 30 days)
   - PIX Events by Generic Alert
   - PIX Events by Severity
   - PIX Events by Category
   - Management Events
5 On the Configurations view tab, expand **Symantec Enterprise Security**.
6 Verify that the following item is listed:
   - Symantec Event Collector for Cisco PIX

     For more information about reports and views, see the *Symantec Enterprise Security Architecture Administrator's Guide*.

Troubleshooting the Event Collector installation

If you are not receiving PIX events after the Symantec Event Collector for PIX installation, perform the following procedures to confirm operation:

Verifying the SESA Manager address and port

Verify that you specified the correct SESA Manager IP address (or host name) and the correct number for the SESA secure directory port when you ran the SESA Integration Wizard.

To verify the SESA Manager address and port on Windows

1 On the Event Collector computer, at the command prompt, change directories to the following folder on the hard drive:

   C:\Program Files\Symantec\SESA\Agent
2 In a text editor, open the configprovider.cfg file.
3 Verify that the following options contain the correct settings for the SESA Manager to which you want to send PIX events:
   - mgmtServer
   - mgmtPort

To verify the SESA Manager address and port on Solaris

1. On the Event Collector computer, log in as the root user.
2. Change directories to the installation folder:
   /opt/Symantec/SESA/Agent
3. In a text editor, open the configprovider.cfg file.
4. Verify that the following options contain the correct settings for the SESA Manager to which you want to send PIX events:
   - mgmtServer
   - mgmtPort

To verify SESA Agent connectivity from the SESA Console

1. In the Symantec management console, on the System tab, click **Organizational Units** > **Default**.
2. Verify that the Event Collector host is listed.
3. Select the host and get properties.
4. Click **Services**.
5. Verify that the SESA Agent is started.

To verify SESA Agent connectivity on Windows

1. On the computer on which you installed the Event Collector, on the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Administrative Tools**.
3. In the Administrative Tools window, double-click **Services**.
4. In the Services dialog box, verify that the SESA AgentStart Service is started. If it is not started, right-click on the service and select **Start**.
5. For command-line verification, open a command window via **Start** > **Run**, type the command, and press **Enter**.
6. Change directory to the SESA Agent:

   ```
   cd c:\Program Files\Symantec\PixCollector\AgtInst
   ```

7. Execute the following command to get statistics on the SESA Agent:

   ```
   java –jar agentcmd.jar –status
   ```

See the sample output below. Note the running status and the SESA Manager URL.

```
SESA Agent status: running
Machine Id:  **********obscured**********
Listening on: 127.0.0.1:8086
SSL: On
SESA Manager URL: https://127.0.0.1:443/sesa/servlet/
Total number of post failures: 0
Outbound Thread State: WAIT
Items in Outbound Queue: 0
Queue Status for ProdId 3000
  Queue is stored in memory
  Flush Size (KB): 50
  Flush Time (sec): 300
  Flush Count: 35
  Spool Size (KB): 100
  Max Queue Size (KB): 2000
  Entries waiting in queue: 0
  Total Events processed: 0
  Total Queue Size (bytes): 0
```

To verify SESA Agent connectivity on Solaris

1. On the computer on which you installed the Event Collector, log in as the root user.
2. Type the following command to list the Event Collector daemon processes:

   `ps -efu root | grep Sym`
3. In the list of processes shown, verify that the following processes are running:
   /opt/Symantec/SESA/Agent/agentd -START
4. Change directory to the installation directory of the SESA Agent:
   cd /opt/Symantec/SESA/Agent
5. Execute the following command to get statistics on the SESA Agent:

   ```
   java –jar agentcmd.jar -status
   ```

See the sample output below. Note the running status and the SESA Manager URL.

```
SESA Agent status: running
Machine Id:  **********obscured**********
Listening on: 127.0.0.1:8086
SSL: On
SESA Manager URL: https://127.0.0.1:443/sesa/servlet/
Total number of post failures: 0
Outbound Thread State: WAIT
Items in Outbound Queue: 0
Queue Status for ProdId 3000
  Queue is stored in memory
  Flush Size (KB): 50
  Flush Time (sec): 300
  Flush Count: 35
  Spool Size (KB): 100
  Max Queue Size (KB): 2000
  Entries waiting in queue: 0
  Total Events processed: 0
  Total Queue Size (bytes): 0
```

Verifying Event Collector operation

You can verify Event Collector operation by confirming that the proper services are running and that there are no error messages in the application log file.

To verify Event Collector operation on Windows

1. On the Event Collector computer, select **Programs** > **Control Panel** > **Services**.
2. In the Services window, verify that the following services are running:
   - Symantec Event Collector for PIX
   - SESA AgentStart Service
3. Close the Services window.
4. Select Event Viewer.

5 In the Event Viewer, examine the Application Log for failure events from the Symantec Event Collector for Cisco PIX.

If you see only success events, the problem probably exists elsewhere.

6 Close the Event Viewer and the Administrative Tools windows.

Uninstalling the Event Collector

Uninstalling the Symantec Event Collector for Cisco PIX also removes the SESA Agent if no other products on the PIX Log Server are using it.

After you uninstall, the Symantec Event Collector for Cisco PIX service (and the SESA AgentStart service, if the SESA Agent is uninstalled) are removed from the Windows Services window (service control manager).

Uninstall the Symantec Event Collector for Cisco PIX using the Microsoft Windows Add/Remove Programs feature.

To uninstall the SESA Cisco PIX Collector on Windows

1 On the Event Collector computer, on the Windows taskbar, click **Start** > **Settings** > **Control Panel**.

2 In the Control Panel window, double-click **Add/Remove Programs**.

3 In the Add/Remove Programs dialog box, click Symantec Event Collector for PIX, then click **Remove**.

4 When you are prompted to remove Symantec Event Collector for PIX from your computer, click **Yes**.

Symantec Event Collector for PIX is removed from the Add/Remove Programs dialog box, indicating that the Event Collector is removed.

To uninstall the SESA Cisco PIX Collector on Solaris using the InstallShield uninstaller program

1 On the Event Collector computer, log in as the root user.

2 Change directory to the PIX Collector installation directory.

3 Type the following command:

```
./_uninst/uninstaller.bin
```

4 Follow the on-screen instructions for the InstallShield Uninstall Wizard.

5 When you are prompted to remove Symantec Event Collector for PIX from your computer, click **Yes**.

6 The Symantec Event Collector for Cisco PIX and the daemon process for the Collector (as well as the SESA Agent if not needed) are removed from the computer.

Note: Directories containing logs and other files modified after the install will remain in the installation directory. It is safe to delete these at this point.

Chapter 3

Using the collector

This chapter includes the following topics:

Viewing reports for the Symantec Event Collector for Cisco PIX

The Symantec Event Collector for Cisco PIX lets you use the Symantec management console to view events that are logged by Cisco PIX.

The SESA integration components that you installed on the SESA Manager include predefined reports for Symantec Event Collector for Cisco PIX events.

The reports that are specific to Cisco PIX events are stored in the Symantec Event Collector for Cisco PIX folder within the Firewall Event Family.

To view reports for the Symantec Event Collector for Cisco PIX

1. Log on to the Symantec management console using a SESA user account with sufficient rights to view SESA configurations.

   The SESA user must belong to a role that has rights to the SESA-enabled Symantec Event Collector for Cisco PIX product.

2. On the Events view tab, expand **Symantec Enterprise Security** > **SESA DataStore** > **Firewall Event Family**.

3. Expand the Symantec Event Collector for Cisco PIX folder.

Table 3-1 describes the reports that are specific to the Symantec Event Collector for Cisco PIX.

Table 3-1 Symantec Event Collector for Cisco PIX reports

Report name	Report format	Description
All PIX Events	Table	Displays all events that are logged by the PIX Collector. This is similar to the PIX Log Viewer Display.
PIX Events (last 8 hours)	Table	Displays all events that are logged by the PIX Collector in the last 8 hours.
PIX Events (last 24 hours)	Table	Displays all events that are logged by the PIX Collector in the last 24 hours.
PIX Events (last 30 days)	Table	Displays all events that are logged by the PIX Collector in the last 30 days.
Management Events	Table	Displays details for firewall management commands (reboot, upgrade, etc.).
PIX Events by Generic Alert	Pie chart	Displays the most frequent Generic Alert codes reported by the PIX Collector. The Generic Alert code is a Symantec normalized code that uniquely identifies a security event.
PIX Events by Severity	Pie chart	Displays the distribution of PIX events by SESA severity level.
PIX Events by Category	Pie chart	Displays the most frequent categories of alerts reported by the PIX Collector. Symantec Generic Alert codes are organized into standard categories.

Customizing event reports

In addition to the reports in the Firewall Event Family and the Symantec Event Collector for PIX folder, you can create customized event reports that display data that interest your organization.

For example, to create a report that shows all connection attempts for a specific address, you can display the All Events report and add a filter that reports the address that you are interested in.

For more information, see the section on creating custom reports in the *Symantec Enterprise Security Architecture Administrator's Guide*.

Configuring the SESA Agent

The SESA Agent uses default logging parameters that are appropriate for most event collection circumstances.

Table 3-2 lists the logging parameters:

Table 3-2 SESA Agent logging parameters

Logging parameter	Default value	Description
Listen IP	127.0.0.1	The IP address on which the SESA Agent listens.
Listen port	8086	The port on which the SESA Agent listens.
Management servlet	EventLogger	Identifies the SESA Management servlet to which the SESA Agent sends messages. Should be changed with caution.
Disconnected mode retry interval	30 minutes	When the SESA Manager cannot be contacted, the retry interval for sending events to the SESA Manager.
Maximum queue size	2000 kb	When an application's queue reaches this size, any subsequent log requests are refused.
App flush size App flush time App flush count	15 seconds 50 kb 35	Agent outbound data is sent to the SESA Manager whenever one of the three triggers is tripped. Note: This applies only to batch events. Direct events are always sent as soon as possible.
App spool size	100 kb	The size in kilobytes of the Event Collector queue that the SESA Agent holds in memory when not able to send the normal queue to the SESA Manager. If the queue exceeds this size and it still needs to grow, the queue is written to disk.
Encrypt config file	false	Controls whether the configuration file that is located at the SESA Agent is encrypted.

You can adjust these parameters from the Configurations view tab of the Symantec management console. For more information, see the section on configuring products in the *Symantec Enterprise Security Architecture Administrator's Guide.*

Viewing information from the Symantec Event Collector for Cisco PIX

To view information from the Symantec Event Collector for Cisco PIX

1. On the Symantec management console Events view tab, in the left pane, expand **Symantec Enterprise Security**.
2. Expand the SESA DataStore: <manager_system_name> folder.
3. Click **Firewall Event Family**.
4. In the left pane, click **Symantec Event Collector for Cisco PIX** > **All PIX Events** to display all the events sent to SESA by the Cisco PIX collector.

Understanding the PIX Ruleset

The <installdirectory>\kb\6.2\FirewallInformation.ini file is a csv formatted file that contains information specific to your firewall that you intend to pass onto SESA via the Event Collector.

The collector uses the InternalInterfaces and ExternalInterfaces parameters to distinguish among inbound, outbound, and internal connections through the firewall.

These parameters assume that there is only a single PIX firewall that is reporting to the logfile read by the collector. If multiple PIX firewalls are reporting to this logfile, list the internal interfaces of all the firewalls on the InternalInterfaces line and the external interfaces of all the firewalls on the ExternalInterfaces line.

Note: If an internal interface of one firewall shares the same name as the external interface of another firewall, or vice versa, list these interfaces as only external.

Table 3-3 describes the information parameters.

Table 3-3 Information Parameters Description

Row Name	Parameter Name, Value (default install)	Parameter Definition
InternalInterfaces	N/A	The name of every internal firewall interface should be defined here. An internal interface is defined as one that is connected to a trusted, private enterprise network. The format of this row is:InterfaceName1,InterfaceName2. For example: InternalInterfaces,inside,accounting. Type **show interface** from the PIX Firewall command line interface for a list of all firewall interfaces. You may enter as many interfaces as necessary.
ExternalInterfaces	N/A	The name and IP address of every external firewall interface should be defined here. An external interface is defined as one that is connected to an untrusted, public network (such as the Internet). The format of this row is: InterfaceName1, InterfaceName2. For example: ExternalInterfaces,outside. Type **show interface** from the PIX Firewall command line interface for a list of all firewall interfaces. You may enter as many interfaces as necessary.
Proxies	N/A	List any proxy servers that may be visible to the firewall. These servers often produce false positives such as port scan events because of their high levels of network activity. The collector rule set filters out such false positives originating from proxy servers identified here.
ManagementHosts	console	Identify all hosts that are authorized to manage this firewall. The hosts should be identified by IP address. The format of this row is: RemoteManagementHosts,Host1,Host2,HostN. You may enter as many hosts as necessary.
Communication Parameters	N/A	This row should never be modified.

Table 3-3 Information Parameters Description

Row Name	Parameter Name, Value (default install)	Parameter Definition
FirewallHosts	test_name,0.0.0.0	List the hostname and IP address of all the firewalls reporting to this collector. Ensure that the host names appear here as they do in the syslog events reported by the firewall. If all firewalls reporting to the collector are identified by IP address in the syslog, it is not necessary to populate this parameter. If a PIX event identifies the firewall by host name, the collector attempts to resolve the host name for an IP address using this information. If this parameter is not populated, then PIX events may be stored in the SESA datastore but discarded by Symantec Incident Manager because they do not contain an IP address. SESA fields intended to store an IP address (such as the Machine IP field) may be populated with a host name.

Understanding rule definitions

Table 3-4 describes the rule definitions.

Table 3-4 Rule definitions

Rule	Definition
Section 1: Successful Traffic Options	The parameters in this section define how the collector processes successful traffic events. Successful traffic is defined as packets that are permitted through the firewall by packet filtering firewalls, successful proxy connections that are established by proxy firewalls, and successful connection events that are reported by these proxies (such as FTP Get and Put commands. **Note:** For the Symantec Event Collector for PIX to process successful traffic, the firewall must be configured to log successful traffic activity.

Table 3-4 Rule definitions

Rule	Definition
REPORT_SUCCESSFUL_INBOUND_TRAFFIC	If this rule is enabled, all successful inbound traffic through the firewall is reported to SESA. Traffic is defined as inbound if the traffic originated on an external firewall interface and is destined for an internal firewall interface. For this reason, it is critical that the firewall's interfaces are defined in the collector's FirewallInformation.ini file.
REPORT_SUCCESSFUL_OUTBOUND_TRAFFIC	If this rule is enabled, all successful outbound traffic through the firewall is reported to SESA. Traffic is defined as outbound if the traffic originated on an internal firewall interface and is destined for an external firewall interface. For this reason, it is critical that the firewall's interfaces are defined in the collector's FirewallInformation.ini file.
REPORT_SUCCESSFUL_INTERNAL_TRAFFIC	If this rule is enabled, all successful internal traffic through the firewall is reported to SESA. Traffic is defined as internal if the traffic originated on an internal firewall interface and is destined for an internal firewall interface. For this reason, it is critical that the firewall's interfaces are defined in the collector's FirewallInformation.ini file.
Section 2: Denied Traffic Options: REPORT_DENIED_INBOUND_TRAFFIC	If this rule is enabled, all denied inbound traffic through the firewall is reported to SESA. Traffic is defined as inbound if the traffic originated on an external firewall interface and is destined for an internal firewall interface. For this reason, it is critical that the firewall's interfaces are defined in the collector's FirewallInformation.ini file.
REPORT_DENIED_OUTBOUND_TRAFFIC	If this rule is enabled, all denied outbound traffic through the firewall is reported to SESA. Traffic is defined as outbound if the traffic originated on an internal firewall interface and is destined for an external firewall interface. For this reason, it is critical that the firewall's interfaces are defined in the collector's FirewallInformation.ini file.
REPORT_DENIED_INTERNAL_TRAFFIC	If this rule is enabled, all denied internal traffic through the firewall is reported to SESA. Traffic is defined as internal if the traffic originated on an internal firewall interface and is destined for an internal firewall interface. For this reason, it is critical that the firewall's interfaces are defined in the collector's FirewallInformation.ini file.

Table 3-4 Rule definitions

Rule	Definition
Section 3: Remote Management Options IGNORE _MANAGEMENT_ FROM_AUTH_ HOSTS	If this rule is enabled, the collector reports only management activity if the remote host is not listed as an authorized management host in the collector's FirewallInformation.ini file. If this rule is disabled, all remote management activity is reported to SESA.
Section 4: Ping Activity Options ROLLUP_ INBOUND_PINGS	This rule defines how ping activity from external hosts should be processed. If set to 0, ping events from external hosts are ignored. If set to 1, every ping event from an external host is reported to SESA. If set to 2 or greater, the collector rolls up ping activity by source IP address. For example, if ROLLUP_INBOUND_PINGS is set to 5, the collector reports every fifth ping event from a given source IP address.
ROLLUP_ OUTBOUND_ PINGS	This rule defines how ping activity from internal hosts should be processed. If set to 0, ping events from internal hosts are ignored. If set to 1, every ping event from an internal host is reported to SESA. If set to 2 or greater, the collector rolls up ping activity by source IP address. For example, if ROLLUP_OUTBOUND_PINGS is set to 5, the collector reports every fifth ping event from a given source IP address.
ROLLUP_ INTERNAL_PINGS	This rule defines how ping activity between internal hosts should be processed. If set to 0, ping events between internal hosts are ignored. If set to 1, every ping event between internal hosts is reported to SESA. If set to 2 or greater, the collector rolls up ping activity by source IP address. For example, if ROLLUP_INTERNAL_PINGS is set to 5, the collector reports every fifth ping event from a given source IP address.
Section 5: Port Scan Options DETECT_PORT_ SCANS	This rule detects port scans from a single source IP address to a single target IP address. If enabled, an event is sent to SESA if a single source IP address attempts to connect to more than PORT_SCAN_THRESHOLD unique ports on a single target IP address within PORT_SCAN_TIMEOUT seconds.
DETECT_PORT_ SWEEPS	This rule detects port sweeps from a single source IP address to multiple target IP addresses. If enabled, an event is sent to SESA if a single source IP address attempts to connect to the same port on more than PORT_SWEEP_THRESHOLD unique hosts within PORT_SWEEP_TIMEOUT seconds.

Table 3-4 Rule definitions

Rule	Definition
Section 6: Authentication options ROLLUP_FAILED_LOGINS	This rule defines how failed login events should be processed. If set to 0, failed login events are ignored. If set to 1, every failed login event is reported to SESA. If set to 2 or greater, the collector rolls up failed login events by user name. For example, if ROLLUP_FAILED_LOGINS is set to 5, the collector reports every fifth failed login event for a given user name.
IGNORE_BUSINESS_HOURS	If this rule is enabled, the SESA severity of certain events (management, system status, and user account activity) that occur outside normal business hours will be increased. Business hours are defined by the BusinessDayBegins and BusinessDayEnds parameters. If this rule is enabled, weekends are always considered outside normal business hours.
NAT_CONNECT_COUNT_THRESHOLD	This rule defines how NAT failed events should be processed. If set to 1, every NAT failed event is reported to SESA. If set to 2 or greater, the collector rolls up NAT failed events. For example, if NAT_CONNECT_COUNT_THRESHOLD is set to 5, the collector reports every fifth NAT failed event.
Section 7: CATCH_ALL	This rule detects all events not evaluated by the previous rules.

About the knowledge base

The Symantec Event Collector for Cisco PIX takes security event information that is gathered by the PIX product and formats it so that the Symantec Enterprise Security Architecture (SESA) can use it. To perform this function, it uses a knowledge base that consists of rule files, translator files, and knowledge base tables.

A rule file is a text file with a .rule extension. The Symantec Event Collector for Cisco PIX rule files contain standard rules that let the collector perform its translations.

Event collectors ship with a filtering rule that prunes excess events, preventing them from appearing in SESA. For information about rules and how they are used, refer to the *Symantec Incident Manager Implementation Guide*. In general, use the event disposition list to ensure maximum effectiveness of the system.

To filter device-specific events, use the DE_CustomerRules.rule file. To filter events with a particular Generic Alert code, copy and paste the rule that is contained within the file. Then replace the ExampleAlert with the Generic Alert code that you want to filter and uncomment the lines. Restart the collector to apply the rule. This rule tells the system to do nothing if it sees the indicated event.

A collector translation file is a text file, with a .trn extension, that consists of one or more translation specifications. Translation specifications are expressions within the translation file that tell the collector how to translate a single type of external message from a data source into a normalized SESA event.

Knowledge base tables use a .kbt extension. They contain information about the events from PIX and how to distribute them. Knowledge base tables also contain information about event categories and event severities. The Symantec Event Collector for Cisco PIX uses the knowledge base files to add interpretation and meaning to the codes that are mapped by the translation files.

Editing knowledge base table files

The Symantec Event Collector for Cisco PIX uses the knowledge base table to match PIX event information to a normalized event table. You can edit the knowledge base table to add your own custom events. For all rules to work properly, you must use predefined generic event codes and categories/subcategories. You can find the normalized event and category tables in a PDF file in the Docs directory of the Installation CD-ROM.

The <installdirectory>\kb\6.2\PIX.kbt file is a csv-formatted file with the parameters that are listed in Table 3-5.

Table 3-5 lists the fields in the Symantec Event Collector for Cisco PIX knowledge base table.

Table 3-5 Symantec Event Collector for Cisco PIX table fields

Field	Description
DeviceAlert	The code that is taken from the device event stream that uniquely identifies the event.
GenericAlert	A generic event code that corresponds to this particular DeviceAlert. For example, different devices from various companies may use different codes to report the same attack. The knowledge base table ensures that the same generic code is used for the same attack.
Category	The generic alert category that describes the event.
Subcategory	The generic alert subcategory that further describes the event.

Table 3-5 Symantec Event Collector for Cisco PIX table fields

Field	Description
Severity	The seriousness of the potential security implications of the event.

To add a new event to the PIX knowledge base table

1. Open the table in any text editor.
2. Type the information for the new event. Separate each field with a comma.
3. Save the table as PIX.kbt.

The following is an example of a correctly entered event:

```
MyEvent,Malicious_BackdoorProbe_traffic,RECON-EVENTS,CONNECT-SCAN,3
```

Index

T

U

V